EXECUTIVE DIRECTIVE NUMBER EIGHTEEN (ED18): VITA GUIDANCE

EXECUTIVE DIRECTIVE NUMBER EIGHTEEN: ENSURING A SAFE WORK PLACE

IT CONTINGENT LABOR CONTRACT (ITCL)

All vendors will be responsible for certifying that their staff augmentation or statement of work (SOW) staff who work on-site or perform public-facing services are 1) fully vaccinated or 2) if not fully vaccinated, are required to wear a mask, maintain social distancing, and adhere to all other agency safety protocols while working on-site or engaged in-person with the public. CAI will begin working immediately with all vendors who have currently engaged contractors to ensure completion of the required attestation

If there are any questions, please contact your VITA customer account manager.

If there are any questions relating to ED18, please contact: the Department of Human Resource Management (DHRM) via email at policy@dhrm.virginia.gov or phone at 804-225-2131.

FACILITY ACCESS FOR VITA SUPPLIERS

Agency information technology resource (AITR) staff have been asked to complete a survey to share their agency's procedures and needs for VITA's suppliers to be aware of and fulfill prior to rendering on-site technology support. The survey asks if an agency has documented procedures in place and asks that a copy of the procedure be uploaded. If no documented procedures are available, agencies should provide a point of contact for suppliers to use.

Survey: Agency access requirements (NOTE: Only AITR staff have access to the survey)

SECURITY GUIDANCE FOR ED18-RELATED DATA STORAGE AND SHARING

No matter what system your agency uses to track vaccination data, do so securely and in compliance with security standards.

See Appendix below for guidance.

APPENDIX

Security guidance for ED18-related data storage and sharing

In accordance with Executive Directive Number 18 and Department of Human Resource Management guidance, and with VITA's information security policies, consider the following when storing and processing data related to vaccination verification for your agency:

1. Agencies should establish a process for COVID-19 vaccine testing verification which includes the following:
    a. Agencies must identify the parties authorized to view vaccine verification and testing related data
    b. Verification data, vaccine verification related documentation and testing data must be treated as sensitive relative to confidentiality and integrity
2. In planning for information security, keep in mind that an individual may provide different types of records to the agency to demonstrate vaccination or testing status:
    a. an original COVID-19 vaccine card/record
    b. a paper copy or facsimile of their COVID-19 vaccine card/record
    c. a digital image or digital photograph of the record
    d. a QR code or database link sourced from the Virginia Department of Health
    e. an official medical provider record (or copy of the record) confirming the vaccination
3. Agencies must take appropriate steps to protect privacy and IT security, while also providing relevant information to those who need to know in order to implement safety protocols. Agencies should consult with their own records officer, privacy officer, ISO, AITR, other senior agency officials, and their counsel as necessary to determine the best means to maintain this information to meet agency needs.
4. When an automated method is used in place of paper forms for collecting vaccine information, it must include a method to disclose to the employee what information is being collected and what it will be used for. In addition, it must include a mechanism to capture the acknowledgement of the employee that the information collected is accurate and true.

5. For information security purposes, an employee's response regarding vaccination is considered private and confidential medical information. That does not necessarily mean that it is protected health information (PHI) or data that is subject to regulations under the Health Insurance Portability and Accountability Act (HIPAA). See SEC525 IR-4-COV-2 for how VITA's security policies define confidential medical information.

6. Any unauthorized access or breach of the vaccination related verification data must be reported to VITA as soon as possible, in accordance with Va. Code § 2.2-603(G).

7. IT guidelines for storing vaccination and testing data: In general, agencies are required to follow and comply with all Commonwealth of Virginia information security policies, practices and standards as defined by SEC-525. Agencies not under the governance of VITA must adhere to the other applicable laws and standards for maintaining secured data.

   The following list some of the more significant IT areas that must be addressed:

   a. Limit the number of authorized users: In general, the agency's human resource office should serve as the primary reviewer and collector of vaccination records. Agencies may delegate this responsibility on a need-to-know basis to meet operational requirements.

      i. If vaccination data will be stored in a network fileshare, ensure only authorized users have access to the folder.

      ii. If vaccination data will be stored in an internal database, ensure that only authorized users can access the database or portion of the database containing vaccination records.

      iii. If vaccination data will be stored by a third-party software as a service solution (SAAS), only SAAS solutions that are approved and managed through VITA's enterprise cloud oversight service (ECOS) can be used.

   b. Use strong user authentication: Consider heightened password security or multifactor authentication.

   c. Encrypt the data: Make data unreadable to anyone except authorized users and intended recipients. This is applicable to stored and transmitted data. Encryption protects the integrity of vaccination documents, images, messages and related information.

   d. Create an audit trail: Track anyone that accesses vaccination data and record any changes or updates to the data.

e. Implement physical safeguards: Protect access to hardware used to share and transfer vaccination data to make sure that only the right people have access to the right areas. Physical safeguard controls include: facility access controls; workstation use and security controls; and device and media controls.

8. Guidelines for securing and storing supporting physical documentation:

a. Agencies must secure physical copies of vaccination records if collected. Agencies must immediately report all incidents that may involve the loss or theft of physical vaccination records.

b. Physical copies of vaccination records, if collected, must be stored in areas with controlled access or in locked cabinets.

c. Physical copies should always be stored out of sight of unauthorized individuals and should be locked in a cabinet or room when not in use.

d. There should be a process for tracking / logging the location of physical vaccination records while in use, transit or storage.

e. If a physical vaccination record is in use, but not actively being viewed, it should be closed, covered or placed in a position to minimize incidental disclosure.

f. If a physical vaccination record is in transit, it must be covered so that no personal identifiers are visible when moving the records.